An Analysis of Record Security Route Using With Message Authentication Code

A Synopsis

Submitted in

Partial fulfillment for the degree

Of

Doctor of Philosophy

(Computer Science)

Supervised by
JV'n Dr. Akash Saxena

Submitted by
JV'n Ms. Neha Sharma

Department of Computer Science & Information Technology

Faculty of Engineering & Technology

Jayoti Vidyapeeth Women's University, Jaipur (Rajasthan)

April, 2014

Introduction:

Transmission path assurance has never been an intricate part of network security before. Due to nature of the Internet Protocol (IP), a data packet will take the shortest path possible and even with a reliable protocol like the transmission Control Protocol (TCP), a packet is only assured delivery, but not the path it had taken to get to the destination. Recording the path of a data packet is useful in auditing the different subnets or network a packet had taken. This is useful information, if there is location sensitivity attached to the packet. Together with the multi-level authentication scheme, authorization has yet another matrix to decide on the access a user has, based on the intermediary networks the data packets traverse.

Another area which benefits from a recorded transmission path is for audit packets. This ensures that the audit packets have a recorded path, so that should any man-in-the-middle attack be used, the attacker can be tracked more easily. This will propose an extension to the IP packet that includes an ad-hoc IP-trailer.

This trailer includes the information regarding the packet transmission on path. The inclusion of such information could aid in the use to fight against online adversaries and can lead to more successful prosecution and also reduction in such activities. The design takes into consideration that the change to IP will be handled by intermediate hops in a network, whether they are compliant to the new design or not. The benefit for this is mainly for forensics purposes, but may be of interest to context-aware authorization, or even the tracking of SPAM on the internet.

Internet Protocol (IP), based on RFC791 is considered to be the most widely used layer 3, networking protocol. Introduced in 1977, the Internet Protocol is a connectionless, unreliable protocol, depending on a best-effort delivery mechanism. This means that should a packet be dropped or lost during transmission, no effort is made to report such an occurrence. The main reason for such a delivery system was because at the same time, the Transmission Control Protocol (TCP) was developed.

The Internet Protocol offers two options to make deterministic transmission path decisions; Strict Source and Record Route (SSRR), and Loose Source and Record Route (LSRR). These options allow for the source of the transmission packet to supply routing information to the intermediary gateways, and also to record the route information. SSRR differs from LSRR in that; the gateway must send the packet to the next address in the source route through only the directly connected network. If such a condition is not met, the packet will be dropped. The options are often not used, mainly because of its impact on traffic congestion explains that enforcing a routing policy on network traffic will inevitably inflate shortest-router-hop path.

The Internet Protocol version 6 (IPv6), RFC2460 has a much simpler construct, but yet more features as compared to IPv4. Most options in the header field were removed, relying on the extensible header feature that makes up for most of the header in an IPv6 header. The Source Route option, though, has been preserved and left in the Routing Header of the new design. IPv6 handles Source Route almost similarly to IPv4, however, more features have

been included. This includes the removal of Strict/Loose source routing, for a more flexible scheme that allows for both modes of routing to be decided upon at every node. The Source Routing feature in IPv6 does not specify for a direct Record Route function like IPv4, but has this feature as part of the Source Route functionality.

One of the main concerns of recording routes in IPv4 and IPv6, is that the field is stored as a plaintext. Any intermediary node has access to it, and can choose to manipulate it in a variety of ways. To protect such a field, an integrity check should be done. The proposed design employs similar technique in protection. Although the two end communicating entities have no direct trust with the intermediary nodes, it trusts that the nodes would participate according to the proposed design, and if not, the receiving entity can detect the disparity.

Security Requirements for secure data in during network access such as

Authentication of Hops- A loose authentication method is needed to ensure that the intermediary hops have participated in the design. Although the two end communicating entities have no direct trust with the intermediary nodes, a noncompliant participation in the route would break the authentication scheme. This shows up as a disparity in the integrity check. The loose authentication method is based on the ability of each routing node to comply with the design.

Integrity of Recorded Routes- The integrity protection of the recorded route is vital. The design should provide a means for verification of the integrity of this list. The two most common methods for providing integrity protection include the use of digital signatures based on public-keys and also Keyed-Hash Message Authentication Codes (HMACs).

Performance v/s Security- The list of recorded routes has to be protected by cryptographic means. Choosing the algorithm is important, because it is assumed that intermediary hops do not possess the computational power of a full-fledged system. The algorithm has to be quick, and lightweight, but yet provides enough protection, to satisfy this requirement.

Objective: -

The present work is undertaken to comparative analysis of record secure route using message authentication code with the following objectives:

1. Security requirements for the proposed design have been specified for message header size.
2. To make enough size of relative header size of message.
3. To control the fragmentations on IP packets.
4. To prevent a strong change of IP protocol.

Review of Literature

Candy Yiu, Suresh Singh, 2011, In this research paper, In typical enterprise networks, a large fraction of ports see utilization of less than 5% at peak times and close to zero utilization otherwise. Therefore, the normal architecture of one switch port per end-host is very wasteful because of the need for high port density switches to support numerous end users. In this paper we propose merging traffic from multiple end-hosts and feeding that to small port density switches that can replace the high port density switches. The energy savings from such a redesign are significant. The innovative part of this paper is the design of a low-power Merge network that is used to merge traffic from N incoming links to be fed to K switch ports and for sending traffic from the K-port switch to N links. Further, we present algorithms to enable network designers to re-architect their networks using the merge network, and a feasibility study using our College of Engineering network as a working example to illustrate how this approach would work and the resultant energy savings of almost 47%.

Candy Yiu, Suresh Singh, 2011, In this research paper, reducing energy consumption in the Internet has become an increasingly important goal recently. Previous work on reducing energy consumption has primarily looked at either changing link rates or putting interfaces to sleep. Due to the unpredictable nature of traffic, the energy savings achieved have been modest, do not scale, and incur losses and delay. This paper proposes a different approach to the problem which involves a new switch architecture combined with a simple sleep/awake algorithm. The main results we obtain are that energy consumption, measured as fraction of interfaces that are awake, scales *linearly* with load for all loads with no delay and very low packet loss. We demonstrate the behavior of the algorithm via detailed simulations using synthetic traffic and traffic traces collected at a LAN switch in our university. We obtain over 90% energy saving in all real traffic traces and zero packet loss.

Yogendra Kumar Jain, Surabhi Singh, Feb 2011, In this research paper, A honey pot is a non-production system, design to interact with cyber-attackers to collect intelligence on attack techniques and behaviors. There has been great amount of work done in the field of network intrusion detection over the past three decades. With networks getting faster and with the increasing dependence on the Internet both at the personal and commercial level, intrusion detection becomes a challenging process. The challenge here is not only to be able to actively monitor large numbers of systems, but also to be able to react quickly to different events. Before deploying a honey pot it is advisable to have a clear idea of what the honey pot should and

should not do. There should be clear understanding of the operating systems to be used and services (like a web server, ftp server etc) a honey pot will run. The risks involved should be taken into consideration and methods to tackle or reduce these risks should be understood. It is also advisable to have a plan on what to do should the honey pot be compromised. In case of production honey pots, a honey pot policy addressing security issues should be documented. Any legal issues with respect to the honey pots or their functioning should also be taken into consideration. In this paper we explain the relatively new concept of "honey pot." Honey pots are a computer specifically designed to help learn the motives, skills and techniques of the hacker community and also describes in depth the concepts of honey pots and their contribution to the field of network security. The paper then proposes and designs an intrusion detection tool based on some of the existing intrusion detection techniques and the concept of honey pots.

Atul Yadav , Parag Joshi, January 2012, In this research paper, A Mobile Ad hoc Network (MANET) is a kind of wireless ad-hoc network, and is a self configuring network of mobile routers connected by wireless links. Self configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. Efficient routing protocols will make MANETs reliable. Various research communities are working in field of MANET and trying to adopt the protocols and technology in other applications as well. In this Seminar, an attempt has been made to compare three well know protocols AODV, DSR and DSDV by using three performance metrics packet delivery ratio, average end to end delay and routing overhead.

Ankur Patel, Shivendu Dubey, Ashok Verma and Sharda Pd. Patel, January 2012, In this research paper, A mobile ad hoc network (MANET) is a collection of wireless mobile nodes forming a dynamic network Topology without the aid of any existing network infrastructure or centralized administration. Each node participating in the network acts as a host and as a router means they have to forward packets and identify route as well. Random waypoint is the most common mobility model in most of the simulation based studies of various MANET routing protocols. The Group Mobility Model has been generated by Impact of Mobility Patterns on Routing in Ad-hoc Network (IMPORTANT). In the present communication, we have analyzed the Packet Delivery Ratio (PDR), Average End to End delay, Average Throughput, Normalized Routing Load (NRL) and number of Drop packets in CBR and TCP traffic models using routing protocols namely AODV and DSDV. Research efforts have focused much in evaluating their performance with same number of nodes but divided in different number of groups. Simulations have been carried out using NS-2 simulator.

Bimal Kumar Mishra, Gholam Mursalin Ansari, *Jan. 2012,* In this research paper, A deferential electronic Susceptible-Infectious-Removed- Susceptible (e-SIRS) epidemic model of virus and worms in a computer network has been formulated. Latent period, immune period and time for self replication have been considered. Stability of the result is stated in terms of the

threshold parameter. We have derived an explicit formula for the reproductive number and have shown that the virus-worm- infection-free equilibrium, whose component of infective is zero, is globally asymptotically stable if threshold number is less than one, and unstable if it is greater than one. Numerical method is employed to solve the system of equations developed and interpretation of the model yields interesting revelations.

ZANG Weihua,GUO Rui, February 2012, In this research paper, Network security situational awareness is a hot research spot in network security field. A quantitative method of network security situational awareness based on evolutionary neural network is proposed, combined with the good global search capability and the classification capability of neural network, in which evolutionary strategy is used to optimize the neural network's architecture in order to improve its classification ability, then realize the extract of the network security situational factors to generate the network security situation graph ultimately.

Jiahong Wang, Yuhiro Yonamine, Takashi Iokawa, Eiichiro Kodama, and Toyoo Takata, March 2012, In this research paper, It was found that in the disaster-hit area, a communication supporting system using the existing mobile ad hoc network techniques cannot function as expected and communication would be interrupted from time to time, since they have not taken into consideration the sleep operation that is a very frequently used means for users of mobile terminals to increase their battery life time. In order to solve the problem, this paper proposes a system model and two methods. The one is used to create a house-watching network taking charge of waking up the sleeping terminals, so that periodic or planned communication can be supported even though users freely get into sleep at their convenience. The other is used to incorporate the sleeping with the routing protocols, so that users' consideration for other people can be technically supported, and they can know if their terminals are functioning as routers, and when sleeping buttons of their terminals can be pushed down safely without interrupting the relaying in progress, and so without interfering with others' communication. These methods have been demonstrated to be effective by simulation experiments.

FaseeUllah, Waqas Tariq, Dr. Muhammad Arshad, Muhammad Saqib, Noor Gul, March 2012, In this research paper, In Computer Network number of security techniques provide security consolation but not up to optimal security extent. There are massive attacks and efficient viruses travel across the network which incapacitates computer system and default configuration of the operating system. Preceding techniques can capture anomalous activates and previous known attacks but unknown Security attacks have learned to survive in a high secure precinct, it must be noticed by every technical person that virus has an augmenting influence, so it is very difficult to detect unknown attacks at application layer on the run time.

Jaya Jacob, V.Seethalakshmi, April 2012, In this research, MANET (Mobile Ad-hoc Network) is a self organizing and self configuring network without the need of any centralized

base station. In MANETs, the nodes are mobile and battery operated. As the nodes have limited battery resources and multi hop routes are used over a changing network environment due to node mobility, it requires energy efficient routing protocols to limit the power consumption, prolong the battery life and to improve the robustness of the system. This paper evaluates the performance of various ad-hoc routing protocols such as DSDV, AODV, DSR, TORA and AOMDV in terms of energy efficiency and it also proposes a new routing algorithm that modifies AOMDV and it provides better performance compared to all the above protocols. Simulation is done using NS-2(version NS-2.34).

Bharat Singh, Parvinder Singh and Dr. V.S. Dhaka, April 2012, In this research paper, Wireless Sensor Network consisting of a large number of sensor nodes that connected through wireless media has emerged as a ground breaking technology that offers unprecedented ability to monitor the physical word accurately. The privacy preservation is an important issue in wireless sensor network. Developing effective security solutions for wireless sensor networks are not easy due to limited resources. In this paper we propose new techniques for the purpose of security in wireless sensor network called as SDEP sensor data encryption protocol. In the scheme we use the RC 6 method for the purpose of encryption and decryption. RC 6 provide best confusion and diffusion properties with the less computational overhead. In order to confirm effectiveness of SDEP, a comparative performance evaluation with AES and RC 5 algorithms are presented in terms of memory requirement and execution time criteria. Our proposed scheme provides better performance than AES and RC 5 in the term of execution time and total memory requirement. We also provide simulation results for proposed method in the term of overhead and energy according to this result SDEP is strong block cipher for wireless sensor networks.

Diwakar Shukla, Kapil Verma, Jayant Dubey and Sharad Gangele, May 2012, In this research paper, Many well-developed countries are having broadband services for their network connection but under developed countries are still having the dial-up-setup connection network. The cyber crime users are growing fast in the entire world and correspondingly the cyber criminals are also growing. The crime is performed by the user's cyber only when the connectivity through internet is made. This paper extends the approach of interrelationship between traffic sharing and blocking probability of network between operators subject to conditions the user attracts for cyber crimes. The Markov chain model based approach provides a complicated relationship. This paper adopts a simplified form of same relationship assuming linearity among variables. Least square method is used to generate linear relationship in presence of cyber crime using coefficient of determination and 99 percents confidence interval it has been proved that the approximation is best.

Alessandro Carrega, Suresh Singh, Roberto Bruschi and Raffaele Bolla, May 2012, In this research paper, Numerous studies have shown that datacenter networks typically see loads of between 5% – 25% but the energy draw of these networks is equal to operating them at maximum load. In this paper, we propose a novel way to make these networks more energy proportional – that is, the energy draw scales with the network load. We propose the idea of traffic aggregation, in which low traffic from N links is combined together to create H < N streams of high traffic. These streams are fed to H switch interfaces which run at maximum rate while the remaining interfaces are switched to the lowest possible one. We show that this merging can be accomplished with minimal latency and energy costs (less than 0.1W) while simultaneously allowing us a deterministic way of switching link rates between maximum and minimum. Using simulations based on previously developed traffic models, we show that 49% energy savings are obtained for 5% of the load while we get an energy savings of 22% for a 50% load. Hence, forasmuch as the packet losses are statistically insignificant, the results show that energy-proportional datacenter networks are indeed possible.

Diwakar Shukla, Kapil Verma, Sharad Gangele, May 2012, In this research paper, While dealing with internet users in the setup of two operators the relationship between traffic sharing and blocking probability is examined by many authors using Markov chain model. Assuming dial-up-setup of connection network and introduction of rest state the mathematical relationship has been modified. This relationship contains many input parameters of the model with special reference to rest state parameter. This paper presents a much simplified form of relationship between blocking probability and traffic sharing under rest state. Because of variation of model parameter there is always an expected change in the equation of straight line. All these changes are average out to get best average linear relationship between traffic sharing and blocking probability. This one is useful for immediate computations of traffic sharing levels when input has variant values.

Tingwen Liu, Yong Sun, Alex X. Liu, Li Guo, and Binxing Fang, June 2012, in this research paper, Regular expression (RegEx) matching has been widely used in various networking and security applications. Despite much effort on this important problem, it remains a fundamentally difficult problem. DFA-based solutions can achieve high throughput, but require too much memory to be executed in high speed SRAM. NFA-based solutions require small memory, but are too slow. In this paper, we propose Regex- Filter, a pre filtering approach. The basic idea is to generate the RegEx print of RegEx set and use it to prefilter out most unmatched items. There are two key technical challenges: the generation of RegEx print and the matching process of RegEx print. The generation of RegEx is tricky as we need to tradeoff between two conflicting goals: filtering effectiveness, which means that we want the

RegEx print to filter out as many unmatched items as possible, and matching speed, which means that we want the matching speed of the RegEx print as high as possible. To address the first challenge, we propose some measurement tools for RegEx complexity and filtering effectiveness, and use it to guide the generation of RegEx print. To address the second challenge, we propose a fast RegEx print matching solution using Ternary Content Addressable Memory. We implemented our approach and conducted experiments on real world data sets. Our experimental results show that RegexFilter can speed-up the potential throughput of RegEx matching by 21.5 times and 20.3 times for RegEx sets of Snort and L7-Filter systems, at the cost of less than 0.2 Mb TCAM chip.

Meenakshi, Vinod Kumar Mishra, Kuber Singh, July 2012, In this research paper, A Mobile Ad-hoc Network (MANET) consists of a number of mobile wireless nodes, the communication between these mobile nodes is carried out without any centralized control. MANET is a self organized and self configurable network where the mobile nodes move arbitrarily. The mobile nodes can receive and relay packets as a router. Routing is a critical issue and an efficient routing protocol makes the MANET reliable. There are two types of features of MANET - absence of fixed infrastructure. & absence of central administration. In this paper we discuss about simulation & comparison of the performance between three types of routing protocols, Table Driven (Proactive), On-Demand (Reactive) & Hybrid Protocol using the NS-2 (2.26) simulation tool. These routing protocols compared in terms of packets delivery ratio, average delay and speed.

Sachin Taluja1, Pradeep Kumar Verma, Prof. Rajeshwar Lal Dua, August 2012, In this research Paper, Network Security concerns with concept of designing a secured network is the most important task in any enterprise or organization development. Securing a network mainly involves applying policies and procedures to protect different network devices from unauthorized access. Servers such as web servers, file servers, mail servers, etc., are the important devices in a network. Therefore, securing these servers is the first and foremost step followed in every security implementation mechanism. This paper work demonstrates the tasks needed to enhance the network security in Linux environment. The various security modules existing in Linux makes it different from other operating systems. we analyzing network packets using the most popular open source network protocol analyzer wire shark and on the basis of analyzing the packet work has been done on writing the script to block/allow the network traffic using IP firewall and after blocking traffic further capturing and analyzing of packets using wire shark.

Amit Kumar Sahu, Dinesh Goyal, Naveen Hemrajani,August 2012, In this research paper, Computer Networking is necessary to human beings. Peoples needed to share ideas, research knowledge, and the way of life to their friends. In the modern time, the role of computer

networks became dreamy. Analyzing, accessing, sharing and storing of data and information are very easy with help of distributing computer networking. Social networking sites look after human communication in a better manner and create platforms for in agreement individuals to share their thoughts and opinions. There is a massive contribution of computer networking apparatus in the progress which we see today. This paper explores different properties for the administration for the distributed computer network environment like techniques for measuring and analyzing the performance. This analysis is precious for computer network administrator, who administrating distribute computer network.

Sumedha Kaushik, Ankur Singhal, December 2012, In this research paper, Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use: Cryptographic techniques; hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured **communication.**

R. Mohan, C. Rajan , Dr. N. Shanthi, December 2012, In this research paper, A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links to form an arbitrary topology without the use of existing infrastructure. In this paper, we have evaluated the performance of two routing protocols Ad-Hoc On-Demand Distance Vector Routing Protocol (DSR-Reactive Protocol) and Destination-Sequenced Distance-Vector (DSDV-Proactive Protocol) based upon different Mobility Models to obtain a Stable Mobility Model for MANET Routing Protocol. For experimental purposes, we have considered four mobility model scenarios: Random Waypoint, Reference Group Point Mobility, Freeway and Manhattan models. These four Mobility Models are selected to represent the possibility of practical application in the future. Performance comparison has been conducted across the varying Node Speed with fixed Network size. Experimental results illustrate that performance of the routing protocol varies across different mobility models.

Siddhartha Singh1, Dr.Naveen Hemrajani, February 2013, In this research paper, A Network which have wireless sensor nodes animatedly form an communication-less network or provisional network without using existing network infrastructure is defined as wireless network .The sensing of information in decisive conditions during the emergency state where the sensor network is deploy is its main importance. Benefit of developing sensor network is

increasing for practical information in physical environment in different applications either manually or randomly. Through this paper, we discuss and evaluate the performance of different network parameters on different topologies based on varying the pause time and keeping the speed constant (node speed) in different terrain areas which is small (1000 m. x 1000 m.), large (2000 m. x 1000 m.) and very large (2000 m. x 2000 m.) using AODV routing protocol and monitoring of critical conditions with the help of important parameters like Packet delivery Fraction, Average End- to- End Delay, Average Throughput, NRL and Packet loss.

Inadyuti Dutt, Soumya Paul, Dr. S.N. Chaudhuri, February 2013, In this research paper, Information security has become one of the most important concerns of the total information technology development process. And all the technologies that are used to support the management and maintenance of most of the enterprise are commonly online. So network security is the subject which is applicable anywhere in the business world. Genetic algorithm is such an algorithm that helps the developer to show their creativity not only in the IT field but also in the other fields like robotics, mechanical etc, especially where we are developing any technology for the first time.

Haixia Zhao, Yaowei Li, Jincheng Shen, Mingchuan Zhang, Ruijuan Zheng, Qingtao Wu, March 2013, In this research paper, Geographical and Energy Aware Routing (GEAR) is an efficient routing protocol in wireless sensor networks (WSN). It behaves well in the face of routing attacks, but it is incapable of defending bogus routing information, Sybil attack and selective forwarding. Aimed at this problem, this paper present a location pair wise keys bootstrap scheme based secure geographical and energy aware routing protocol (SGEAR). SGEAR adapted to WSN very well. Then we give the performance analyses of SGEAR. Our performance analyses show that our scheme is efficient to defend above-mentioned attacks.

Mojtaba GhanaatPisheh Sanaei, Ismail Fauzi Isnin, Majid Bakhtiari, June 2013, In this research paper, Today's Mobile Ad hoc Networks (MANETs) became a popular issue for scientists, and diverse studies have been made to increase the performance of ad hoc networks. In MANET nodes compromise to forward packets for each other communicate beyond their transmission range. The mobile nodes communicate with each other without any infrastructure. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks called Wormhole Attack that two adversary node collaborate together to transmit the packets in out of band channel. In this paper, performance of Ad hoc on-Demand Distance Vector (AODV) Protocol and Dynamic Source Routing (DSR) protocol are evaluated in presence of wormhole attack and without wormhole attack with Constant Bit Rate (CBR) traffic under dissimilar scalable network mobility. Also we evaluate effect and compare it with standard protocol in term of Packet Delivery Ratio, throughput and End to End Delay via simulation, using Network Simulation2 (NS2) for our research.

Junxian Huang, Feng Qian, Yihua Guo, August 2013, In this research paper, With lower latency and higher bandwidth than its predecessor 3G networks, the latest cellular technology 4G LTE has been attracting many new users. However, the interactions among applications, network transport protocol, and the radio layer still remain unexplored. In this work, we conduct an in-depth study of these interactions and their impact on performance, using a combination of active and passive measurements. We observed that LTE has significantly shorter state promotion delays and lower RTTs than those of 3G networks. We discovered various inefficiencies in TCP over LTE such as undesired slow start. We further developed a novel and lightweight passive bandwidth estimation technique for LTE networks. Using this tool, we discovered that many TCP connections significantly under-utilize the available bandwidth. On average, the actually used bandwidth is less than 50% of the available bandwidth. This causes data downloads to be longer, and incur additional overhead.

We found that the under-utilization can be caused by both application behavior and TCP parameter setting. We found that 52.6% of all downlink TCP flows have been throttled by limited TCP receive window, and that data transfer patterns for some popular applications are both energy and network unfriendly. All these findings highlight the need to develop transport protocol mechanisms and applications that are more LTE-friendly.

Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Joreta Jetcheva, November 2013, In this research article, An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple networks "hops" may be needed for one node to exchange data with another across the network. In recent years, a variety of new routing protocols targeted specifically at this environment have been developed. But little performance information on much protocol and no realistic performance comparison between them is available. This paper presents the results of a detailed packet-level simulation comparing four multi-hop wireless ad hoc network routing protocols that cover a range of design choices: DSDV,TORA,DSR and AODV. We have extended the ns 2 network simulator to accurately model the MAC and physical-layer behavior of the IEEE 802.1I wireless LAN standard, including a realistic wireless transmission channel model, and present the results of simulations of network 50 mobile nodes.

Mahsa Teymourzadeh, Roshanak Vahed, Soulmaz Alibeygi, Narges Dastanpor, December 2013, In this research paper, A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. In addition, Wireless Sensor networks is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges

wireless sensor networks face today is security. This has been enabled by the availability for a kind of possible attacks; the innate power and recall limit of sensor nodes earn customary security solutions unfeasible. These sensors are equipped with wireless interfaces with which they can communicate with one pther to form a network. In this paper we present a survey of security issues in WSNs, address the state of the art in research on sensor network security, and discuss some future directions for research.

Xin Jin, Li Erran Li, Laurent Vanbever, and Jennifer Rexford, December -2013,In this article, Cellular core networks super from inedible and expensive equipment, as well as from complex control-plane protocols. To address these challenges, we present Soft Cell, a scalable architecture that supports _ne-grained policies for mobile devices in cellular core networks, using commodity switches and servers. Soft Cell enables operators to realize high-level service policies that direct trace through sequences of middle boxes based on subscriber attributes and applications. To minimize the size of the forwarding tables, Soft Cell aggregates trace along multiple dimensions the service policy, the base station, and the mobile device at deferent switches in the network. Since most trace originates from mobile devices, Soft Cell performs _ne-grained packet classification at the access switches, next to the base stations, where software switches can easily handle the state and bandwidth requirements. Soft Cell guarantees that packets belonging to the same connection traverse the same sequence of middle boxes in both directions, even in the presence of mobility. We demonstrate that Soft Cell improves the scalability and edibility of cellular core networks by analyzing real LTE workloads, performing micro-benchmarks on our prototype controller as well as large-scale simulations.

Menaka Sivakumar1, M. K. Jayanthi, January 2014, In this article, The prime haracteristics of Mobile Ad Hoc Network (MANET) are infrastructure free, absence of centralized authority and dynamic nature of nodes which are more vulnerable to security attacks. Reliability and security are prime issues to protect the information and nodes in a network during communication which has received more research interest in designing a dynamic secured routing scheme. QoS is set of service requirement that needs to be satisfied by the network during the data transmission in the network. From the perception of QoS best effort protocols ensure optimum network operation in an unpredictable mobile environment. The multimedia applications are intolerable towards delay and reliability which are the features of mobile network; hence the potentials of MANET were not utilized in multimedia applications. These issues of delay and reliability of packet transmission in MANET are contributed by the stability of the communication link even during the mobility of the nodes. This necessitates analyzing the performance of various secured routing protocols based on the stability of the communication link in case of mobility of nodes during data transfer. The present study is

focused on the comparative analysis on the various secured reactive routing protocols in MANET signifying the connectivity stability during the mobility of the nodes.

Dr. Abdul-Bary, R. Sulaiman, Omar Kh. Salih Alhafidh, March 2014, In this research paper, The recent evolutions of IP networks are seeing IP applications becoming more complex and requiring higher bandwidth consumption. More recently, IP networks are employing MPLS which is a technique can be used to improve the performance of IP networks. By use of MPLS, data packets can be switched on the basis of labels rather than routed on the basis of destination address. MPLS supports different features like traffic engineering (TE), QoS and VPNs etc. The key feature of MPLS is its TE, which plays a vital role for minimizing the congestion by efficient load balancing and management of the network resources. Due to lower network delay, efficient forwarding mechanism, enhancing the speed of packet transfer, scalability and predictable performance of the services provided by MPLS technology makes it more suitable for implementing real-time applications such as VoIP and video Conferencing. This paper evaluated the performance measures such as delay variation, delay, page response time, throughput, and packet drop for different types of traffic (voice, video, data) in their movement in a congested network for both MPLS-TE and conventional IP network. OPNET modeler is used to simulate the both networks, the simulation study is conducted in this paper, it is a means to illustrate the benefits of using MPLS-TE for multimedia applications.

K. Pazhanisamy, Dr. Lathaparthiban, March 2014, In this research paper, Security in MANET is the most vital concern for the basic functionality of network. One of the most important challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different type of mechanisms has been proposed using different cryptographic techniques to countermeasure the routing attacks against MANET. We have taken VBOR as the base protocol. The VBOR protocol consists of two phases namely, Route maintenance and Route discovery with the use of variable bit rate. In this paper proposed the message authentication code is generated during route discovery phase then these data are exchanged between the nodes. In VBOR and MAC algorithm is to provide more security in route discovery and data are exchanged to the MANETs.

Methodology

This research deals with the methodological steps adopted in the research study. The research procedures followed are described under the following headlines:

- **A.** Selection of abstract wireless secure route
- **B.** Selection of abstract route methods
- **C.** Use of Tools in research study such as for recording routes in IPv4 and IPv6, RFC versions
- **D.** Behavior of secure route will be examined
- **E.** Implementation in secure route using records

References

1. Alessandro Carrega, Suresh Singh, Roberto Bruschi and Raffaele Bolla, "Traffic Merging for Energy-Efficient Datacenter Networks", IEEE Communications Society, May 2012.
2. Amit Kumar Sahu, Dinesh Goyal, Naveen Hemrajani, "Performance Analysis of Distributed Computer Network over IP Protocol", International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 3– No.8, August 2012.
3. Ankur Patel, Shivendu Dubey, Ashok Verma and Sharda Pd. Patel, "Group Mobility Model Based Proactive and Reactive Routing Protocol in MANET", *International Journal of Electronics and Computer Science Engineering,* ISSN- 2277-1956, V1N4, PP: 2377-2386, January 2012.
4. Atul Yadav , Parag Joshi, "Performance of Flat Routing Protocols in MANET", *International Journal of Electronics and Computer Science Engineering, ISSN- 2277-1956,* V1N4, PP: 2035-2041, , January 2012.
5. Bharat Singh, Parvinder Singh and Dr. V.S. Dhaka, "Sensor Data Encryption Protocol for Wireless Network Security", Global Journal of Computer Science and Technology Volume 12 Issue 9 Version 1.0 April 2012 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. **(USA)** Online ISSN: 0975-4172 & Print ISSN: 0975-4350.
6. Bimal Kumar Mishra, Gholam Mursalin Ansari, "Di®erential Epidemic Model of Virus and Worms in Computer Network", International Journal of Network Security, Vol.14, No.1, PP.88-94, Jan. 2012.
7. Candy Yiu, Suresh Singh, "Merging Traffic to Save Energy in the Enterprise" Portland State University. Portland, 2011.
8. Candy Yiu, Suresh Singh, "Energy-Conserving Switch Architecture for LANs" IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011.
9. Diwakar Shukla, Kapil Verma, Jayant Dubey and Sharad Gangele, "Cyber Crime based Curve Fitting Analysis in Internet Traffic Sharing in Computer Network", *International Journal of Computer Applications (0975 – 8887) Volume 46– No.22, May 2012.*
10. Diwakar Shukla, Kapil Verma, Sharad Gangele, "Least Square Curve Fitting Applications under Rest State Environment in Internet Traffic Sharing in Computer Network",

International Journal of Computer Science and Telecommunications, ISSN 2047-3338, Vol. No. 3, Issue No. 5,PP: 43-51, May 2012.

11. Dr. Abdul-Bary, R. Sulaiman, Omar Kh. Salih Alhafidh, "Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering", International Journal of Computer Networks and Communications Security, ISSN 2308-9830, Vol. No.. 2, Issue No. 3, March 2014.

12. FaseeUllah, Waqas Tariq, Dr. Muhammad Arshad, Muhammad Saqib, Noor Gul, "Analysis of Security Techniques for Detecting Suspicious Activities and Intrusion Detection in Network Traffic", IJCSI International Journal of Computer Science, ISSN (Online): 1694-0814, Vol. 9, Issue 2, No 1,PP: 259-265, March 2012.

13. Haixia Zhao, Yaowei Li, Jincheng Shen, Mingchuan Zhang, Ruijuan Zheng, Qingtao Wu, "A New Secure Geographical Routing Protocol Based on Location Pair wise Keys in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0784, Vol. No. 10, Issue No. 2, PP:365-372, March 2013.

14. Inadyuti Dutt, Soumya Paul, Dr. S.N. Chaudhuri, " Implementation of Network Security using Genetic Algorithm", IJARCSSE, ISSN: 2277 128X,Volume 3, Issue 2, PP: 234-241, February 2013.

15. Jaya Jacob, V. Seethalakshmi, "Performance Analysis and Enhancement of Routing Protocol in Manet", International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Vol.2, Issue.2, pp-323-328 Mar-Apr 2012.

16. Jiahong Wang, Yuhiro Yonamine, Takashi Iokawa, Eiichiro Kodama, and Toyoo Takata, "An Approach to Creating and Maintaining House-Watching Network in MANET", Procedding of the international multiconference of engineers and computer scientists 2012, vol. I,IMECS 2012, march 14-16 2012, Hong- Kong.

17. Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Joreta Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc NeWork Routing protocols", November 2013 MOBICOM , Dallas Texas USA.

18. Junxian Huang, Feng Qian, Yihua Guo,Yuanyuan Zhou, Qiang Xu,Z. Morley Mao, Subhabrata Sen, Oliver Spatscheck, An In-depth Study of LTE: Effect of Network Protocol and Application Behavior on Performance *SIGCOMM'13,* August 12–16, 2013, Hong Kong, China.

19. K.Pazhanisamy, Dr. Lathaparthiban, "Secure Route Discovery in Mobile Ad-Hoc Network Using MAC Based Group Key Management Protocol" International Journal of Advanced Research in Computer Science & Technology (IJARCST), ISSN : 2347 - 8446 (Online),Vol. No. 2, Issue Special No.1, PP: 109-113, Jan-March 2014.

20. Mahsa Teymourzadeh, Roshanak Vahed, Soulmaz Alibeygi, Narges Dastanpor, "Security in Wireless Sensor Networks: Issues and Challenges", ISSN 2308-9830, VOL.1, NO.7, PP: 329–334, December 2013.

21. Meenakshi, Vinod Kumar Mishra, Kuber Singh, "Simulation & Performance Analysis of Proactive, Reactive & Hybrid Routing Protocols in MANET", IJARCSSE, ISSN: 2277 128X, Volume No. 2, Issue No.7, July 2012.

22. Menaka Sivakumar1, M. K. Jayanthi, "Reliability Analysis of Link Stability in Secured Routing Protocols for MANETs" ENGINEERING JOURNAL, DOI: 10.4186, Vol. No.18, Issue No. 1, January 2014.

23. Mojtaba GhanaatPisheh Sanaei, Ismail Fauzi Isnin, Majid Bakhtiari, "Performance Evaluation of Routing Protocol on AODV and DSR under Wormhole Attack", International Journal of Computer Networks and Communications Security, ISSN 2308-9830, VOL. 1, NO. 1, June 2013.

24. R. Mohan, C. Rajan , Dr. N. Shanthi, " A Stable Mobility Model Evaluation Strategy for MANET Routing Protocols", IJARCSSE, ISSN: 2277 128X, Volume 2, Issue 12, PP: 58-65, December 2012.

25. Siddhartha Singh1, Dr. Naveen Hemrajani, "Performance Evaluation of AODV Routing Protocol in Wireless Sensor Networks with the Constraints of varying terrain areas by varying pause time", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. No: 2, Issue No.1, ISSN 2278-6856, February 2013.

26. Sachin Taluja1, Pradeep Kumar Verma, Prof. Rajeshwar Lal Dua, "Network Security Using IP firewalls" IJARCSSE, ISSN: 2277 128X, Volume 2, Issue 8, PP: 338-354, August 2012.

27. Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques", IJARCSSE, ISSN: 2277 128X, Volume 2, Issue 12, PP: 105-107, December 2012.

28. Tingwen Liu, Yong Sun, Alex X. Liu, Li Guo, and Binxing Fang, "A Pre filtering Approach to Regular Expression Matching for Network Security Systems" Applied Cryptography and *Network* Security, June 2012,

29. Xin Jin, Li Erran Li, Laurent Vanbever, and Jennifer Rexford, "Soft-Cell: Scalable and Flexible Cellular Core Network Architecture", CoNEXT'13, December 9-12, 2013, Santa Barbara, California, USA..

30. Yogendra Kumar Jain, Surabhi Singh, "Honeypot based Secure Network System", International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397 Vol. 3 No. PP: 612-6202 Feb 2011.

31. ZANG Weihua,GUO Rui, "The Application of Neural Network based on Evolutionary Strategy in Network Security Quantification Analysis", Advances in information Sciences and Service Sciences(AISS), Vol No:4, Issue No: 2, February 2012.